อนิวรรถน์ สมาธิวัฒน์

ผ่าแผนปฏิบัติการ Registry หัวใจของวินโดวส์ ภาค 3

ความมหัศจรรย์ของ Registry
นั้นมีอยู่มากแต่ถ้ารู้ถึงแก่นลึกของตัว Registry
แล้วการควบคุมใน Windows ก็ไม่ใช่เรื่องยากอีกต่อไป

Windows registry

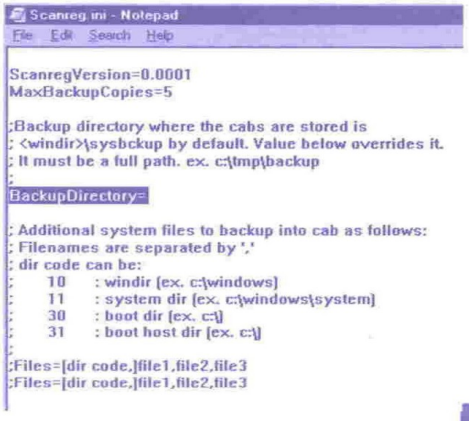
Registry กับ ini ไฟล์

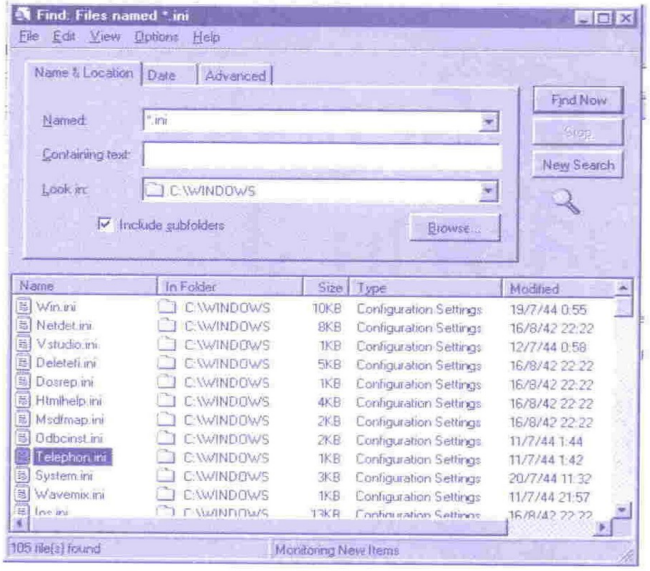
ในบทความฉบับที่ 191 ผู้เขียนได้พูดถึงไมโครซอฟท์ที่พยายามจะยกเลิกไฟล์ ini และย้ายมาไว้ใน Registry แทน ความจริงไมโครซอฟท์ยังจำเป็นต้องมีไฟล์อย่างน้อย 2 ไฟล์ คือ ไฟล์Win.ini และ ไฟล์system.ini เพื่อทำให้ Win9x สามารถสนับสนุนโปรแกรมประยุกต์รุ่นเก่าที่รันบน Windows 3.1ได้ ส่วนไฟล์ ini นี้อยู่ในรูปของไฟล์ข้อความธรรมดาที่สามารถเปิดขึ้นมาด้วยโปรแกรม Notepad ถึงแม้จะมีไฟล์ Registry แล้วก็ตามไฟล์ ini ยังคงมีเห็นใช้อยู่บ้างด้วยเหตุผลต่าง ๆ ดังนี้

- สำหรับใช้งานเพื่อให้สนับสนุนกับบางส่วนในวินโดวส์ที่ยังเป็น 16 บิตอยู่ เช่น ไฟล์ telephon.ini เพื่อให้สามารถ Compatible กับ TAPI ในโปรแกรมรุ่นเก่าได้

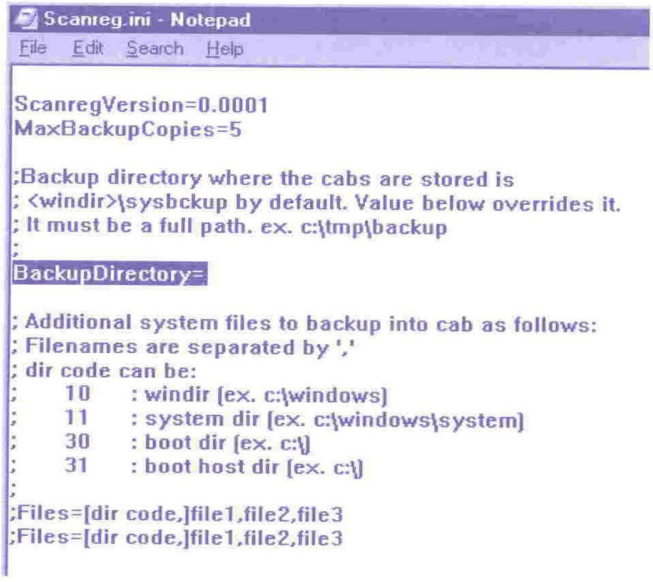
-บางไฟล์ เช่น desktop.ini จะมีอยู่หลายไฟล์ โดยมีข้อมูลภายในที่ไม่เหมือนกันเพื่อปรับค่า config ของโฟล์เดอร์ที่แตกต่างกันออกไป

- บางกรณีไฟล์ ini ถูกใช้แบบ Real mode บน DOS (แต่ชื่อไฟล์ ini เหมือนกัน) เช่น ScanReg.ini ใช้สำหรับปรับแต่งค่าการ Scandisk สามารถเปิดลูกเล่นการทำงานแบบปกติได้และจะไม่สามารถเข้าถึงได้โดยการใช้เมนูในโปรแกรมได้ตามปกติ

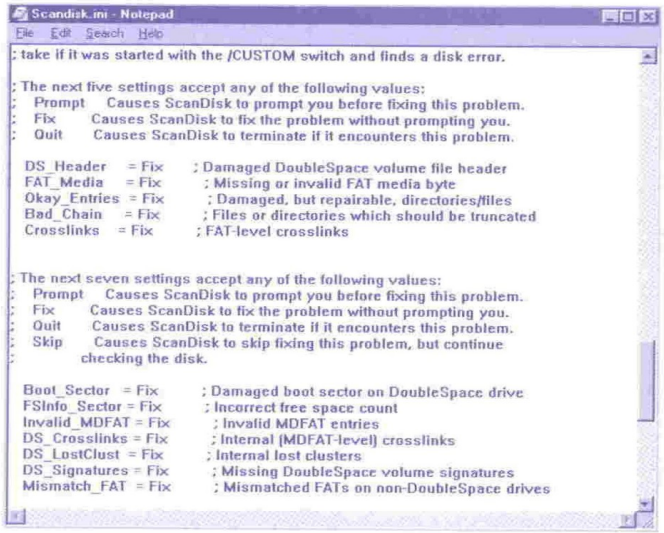




*รูปที่ 1 เมื่อลองค้นโดยใส่ค่า *.ini ลงใน Find file ของ Windows explorer ที่ c:\windows จะพบไฟล์ ini เป็นจำนวนมาก เพื่อสนับสนุนส่วนของ Windows ที่ยังไม่เป็น 32 บิต*



รูปที่ 3 โปรแกรม ScanReg ใช้ไฟล์ ScanReg.ini เพื่อตั้งค่า Configuration ซึ่งอธิบายรายละเอียดของการตั้งค่าอยู่แล้วในไฟล์ จึงกล่าวเพียงจุดที่น่าสนใจ ได้แก่ "MaxBackupCopies=5" ตรงนี้กำหนดจำนวน Registry ชุดสำรอง ถ้าตั้งค่าน้อยกว่านี้ ก็จะมี Registry สำรองน้อย เวลา Registry และถ้าใช้การไม่ได้ จะเสี่ยงมากกว่า แต่หากตั้งค่าไว้มากเช่น 10 ก็จะเปลืองเนื้อที่ Harddisk มาก นอกจากนี้ยังมี "BackupDirectory=" เพื่อกำหนดสถานที่จัดเก็บ Registry ชุดสำรองได้



รูปที่ 2 คุณสามารถปรับแก้ค่าในไฟล์ scandisk.ini ซึ่งไม่ยาก เพราะมีคำอธิบายอยู่แล้วเป็นภาษาอังกฤษ โดยส่วนของ Comment จะอยู่หลังเครื่องหมายเซมิโคลอน (;) โดยโปรแกรมจะไม่มอง ตัวอักษรที่อยู่หลังเครื่องหมายนี้เป็นค่าสั่งเมื่อผู้อ่านปรับแก้ค่าในไฟล์ก็สามารถจะกำหนดให้โปรแกรทำงานได้ ความสามารถที่มากกว่า เพราะความสามารถบางอย่างไม่ได้ถูกออกแบบมาให้เป็นเมนูกดเลือกได้ จึงต้องแก้ค่าคอนฟิกส่วนนี้เองตามตัวอย่างคุณสามารถกำหนดการใช้เมาส์ แสดงผลทางหน้าจอ และตั้งค่าการ Scan การ Fix ปัญหา และการตัดสินใจว่าจะให้โปรแกรมจัดการอย่างไรกับปัญหาที่เกิดขึ้น

- ใช้ในการเก็บค่าเกี่ยวกับระบบเครือข่าย เช่น protocol.ini เก็บค่าระบบเครือข่ายที่ได้ปรับแต่ง

- ไฟล์ win.ini และ system.ini ใช้สำหรับเพื่อให้ Win 9x สนับสนุนโปรแกรมที่รันบน Windows รุ่นเก่าได้ และยังถูกใช้ในกรณีพิเศษ เนื่องจาก ไฟล์ทั้งสองอยู่ในรูป text ไฟล์ จึงสามารถเข้าถึงได้โดยไม่จำเป็นต้องผ่าน Windows ก่อน ส่วนแบบ Registry ทำให้โหลดได้ใน DOS และช่วยให้โหลด Windows ในWindows ได้เร็วขึ้น

ในไฟล์ Win.ini และ system.ini จะเห็นว่ามีเครื่องหมาย bracketed heading " [ ]" อยู่ ส่วนนี้มีไว้กำหนดหมวดหมู่ของค่า config ซึ่งใน Win 98 ได้ย้ายไปเป็น Key ใน Registry นั่นเอง ซึ่งทำให้ความสามารถของระบบมีมากขึ้น เพราะใน ini นั้น ค่าที่อยู่ในไฟล์ เป็นแค่ข้อความ แต่ใน Registry นั้น มีความสามารถมากกว่า เช่น สามารถกำหนดค่าเป็น Execute code ได้

กู้ระบบ Registry

บ่อยครั้งที่ Registry เกิดเสียหาย หากเสียหายน้อยสามารถซ่อมแซมได้ แต่หากเสียหายมากก็ต้องกู้ Registry ขึ้นมา บางครั้งหากเสียหายมากจริง ๆ ก็ไม่สามารถกู้ Registry ได้ จึงจำเป็นต้องมีวิธีการเพิ่มขึ้นมาก็คือการสำรอง Registry

อาการของ Registry มีปัญหาขึ้นอยู่กับลำดับตามความรุนแรง จากมีปัญหาน้อยไปจนถึงมีปัญหาขั้นรุนแรงได้ เช่น

1. Registry หย่อนสมรรถภาพ เกิดจากติดตั้งโปรแกรมมากเกินไป ถอนโปรแกรมแต่ไฟล์ โดยไม่ได้มีการถอน Key อย่างถูกต้อง ใน Registry ถ้าปล่อยไว้นาน ๆ เข้า Registry จะใหญ่ และมีคีย์ขยะที่ไม่ได้ใช้อยู่มากซึ่งส่งผลให้ Load โปรแกรม และ Windows ช้า วิธีนี้ อาจแก้โดยใช้ Utilities เข้ามาช่วย เช่น Registry clean ใน Cleansweeper (กล่าวถึง Utilities นี้ในตอนท้าย) ซึ่งจะช่วยกำจัดคีย์ขยะให้น้อยลงหรือหมดไป

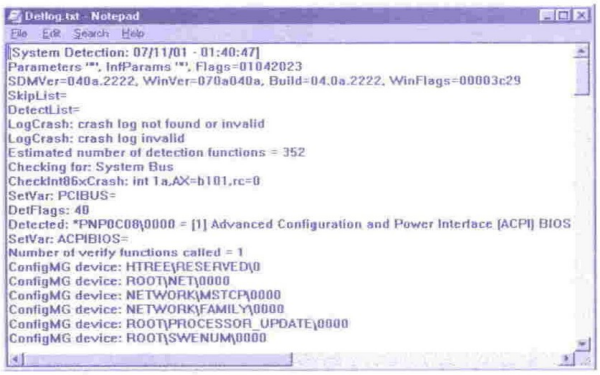
2. Registry ทำให้ Windows เกิด Error แต่ยังสามารถใช้งานได้ เนื่องจาก Registry จะแสดงอาการเสียให้ผู้อ่านเห็นก็ต่อเมื่อ Registry นั้น ๆ มีการเรียกใช้ Device หรือไฟล์ และเมื่อหาไม่เจอก็แสดงอาการออกมา ดังนั้นหากเสียในส่วนของ Windows เอง ผู้อ่านจะสังเกตได้ว่าจะแสดงอาการตั้งแต่ตอน Boot หรือ Load Windows แต่หากเป็นอาการเสียของ Registry โปรแกรมก็จะแสดงตอนเปิดโปรแกรม หรือเมนูนั้น ๆ ผู้อ่านต้องทราบลำดับขั้นตอนในการโหลด Windows ขึ้นมาก่อน

1. จ่ายไฟเข้าเครื่อง การ์ด VDO ทำงานแสดงผลออกทางจอภาพ ตรวจสอบหาการ์ด และ Hardware ต่าง ๆ ในเครื่อง จากนั้นก็เริ่มกระบวนการ POST

2. ค้นหา Boot Sector และโหลดระบบปฏิบัติการขึ้นมา

3. เปลี่ยนไปยัง Protect Mode 32 bit

4.ตรวจสอบ Hardware และ Plug & Play ในระบบ ถ้าเจอก็ให้แก้ไขเข้าไปใน Registry จะแสดง Logo Windows ระหว่างรอ ถ้าเจอ Hardware หรือ Driver ตัวไหนก็ให้บันทึกไว้ในไฟล์ "detlog.txt"



รูปที่ 4

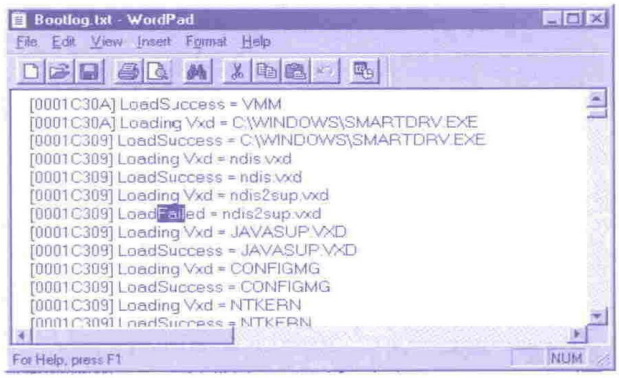
5. โหลด Driver สำหรับ Hardware และปรับแต่งค่าระบบต่าง ๆ ตามที่กำหนดใน system.ini และ Registry

6. เปลี่ยนโหมดแสดงผลเป็นกราฟิก และถ้าขึ้นหน้าจอ Windows ก็วาดไอคอนต่าง ๆ โหลด Wall paper ขึ้นมา

กรณีที่ Windows กำลังโหลดอยู่ในช่วงก่อนขั้นตอนที่ 5 อาการเสียอาจแสดงออกมา โดยข้อความจะปรากฏ Error VKD , Error VXD หรือ Error อื่น ๆ ถ้าหน้าจอสีดำ ข้อความสีขาว บางทีก็บอกชื่อไฟล์หรือ Key ทำให้เกิดปัญหามาให้ด้วยให้บันทึกไว้ก่อน ผู้อ่านสามารถแก้ไขด้วยการเข้า Windows ให้สำเร็จก่อน จากนั้นเปิด Regedit และเลือก Menu Find เพื่อค้นหาคีย์ หรือ Value แล้วใส่ชื่อไฟล์ที่ missing พอเจอแล้วก็ลบ Value นั้นทิ้งไป ลอง Restart เครื่องแล้วดูว่าข้อความนั้นหายไปหรือยัง บางที Value เดียวกันนั้นอาจจะมีอยู่หลายที่ใน Registry ก็ได้ ไม่จำเป็นต้องมีที่เดียว

หาก Windows เปลี่ยนเข้าสู่โหมดกราฟิกแล้ว จะแสดง Error โดยเป็น Dialog box หรือกรอบข้อความให้ผู้อ่านกด OK ให้ผู้อ่านจดชื่อไว้ก่อน แล้วใช้ Regedit แก้เหมือนกัน จากนั้นก็ Restart เมื่อแก้หมดแล้ว ก็ทำการ Clean registry

3. กรณี Registry เสียหายจน Load Windows ไม่สำเร็จ ใน Windows จะมี Safe mode มาให้ด้วย ซึ่ง Safe mode ก็คือโหมดการทำงานแบบปลอดภัย ในโหมดนี้ Windows จะมีการโหลดเฉพาะ Device เบื้องต้นโดยยังไม่โหลด Driver เฉพาะขึ้นมา รวมทั้ง CD-ROM, LAN จะทำการโหลดให้น้อยที่สุด เท่าที่จำเป็นจะทำให้โอกาสที่จะโหลด Windows ได้สำเร็จนั้นมีสูงมาก เพราะหาก Windows โหลด Device ตัวใด แล้วไม่สำเร็จก็จะขึ้น Error เตือน และส่วนใหญ่ก็จะทำให้ Hang ตั้งแต่ขั้นตอนการโหลด ผู้อ่านคงเคยเห็นว่าเวลาที่โหลด windows ไม่สำเร็จ ก็ Reset เครื่อง ครั้งต่อมา Windows จะให้ผู้อ่านเข้าสู่ Safe mode ซึ่งวินโดวส์จะจำค่านับตั้งแต่ขั้นตอนสุดท้ายที่สะดุดเอาไว้ในไฟล์ bootlog.txt (เก็บอยู่ที่ Root directory)



รูปที่ 5

ถ้าสำเร็จก็จะบันทึกว่า Load success เช่น "[0001C28A] LoadSuccess = C:\WINDOWS\DBLBUFF.SYS" แต่ถ้าไม่สำเร็จก็จะบันทึกไว้ว่า LoadFail เช่น "[0001C309] LoadFailed = ndis2sup.vxd" ตรงนี้ทำให้ Windows รู้ว่า Driver หรือ Device ไหนที่ใช้ไม่ได้ ก็จะยกเลิก และในการ Load ระบบปฏิบัติการครั้งต่อไปก็จะผ่าน ดังนั้น Safe mode จึงแก้ไขให้ผู้อ่านโดยอัตโนมัติ โดยไม่ต้องรู้อะไรเลย แค่เข้า Safe mode ให้จบ จากนั้นก็ Shut down

และ Boot เครื่องใหม่ก็จะหาย อย่างไรก็ตาม บางครั้งแม้จะเข้า Safe mode แล้ว ก็ยังไม่สามารถแก้ไขปัญหาได้ ตรงนี้คงต้องเข้าไปแก้ Registry ด้วยตัวเองใน DOS MODE ก็โดยอาศัยโปรแกรม Scanreg /Fix ดังที่เคยกล่าวในฉบับ 191 ผู้เขียนใช้วิธีเหล่านี้อยู่เป็นประจำ และได้ผลดีกว่าหลาย ๆ คนที่ต้อง Format ลงโปรแกรม Windows ใหม่ และในการนำ Registry ชุดสำรองมาใช้นั้น หาก Registry เสียหายจนไม่สามารถ Load Windows ขึ้นมาได้ ก็ต้องแก้กันที่ DOS จึงมีความจำเป็นต้องใช้ Regedit บน DOS ซึ่งก็ได้กล่าวถึงในฉบับที่แล้วเช่นกัน

ให้สังเกตว่า บางที Error อาจจะเกิดกับ Hardware ก็ได้จะส่งผลให้ Load Device ไม่สำเร็จได้เช่นกัน ตรงนี้แตกต่างกันไปแต่ละกรณี อยากให้ผู้อ่านลองสังเกตและเก็บประสบการณ์นี้ด้วยตัวเอง

4. Registry เสียจนไม่สามารถแก้ไขได้ ในกรณีนี้ผู้อ่านต้องอาศัยชุดสำรอง ซึ่ง Windows มีให้อยู่แล้วโดยอัตโนมัติ ทุกครั้งที่ผู้อ่าน Restart เครื่อง Windows จะทำการสำรองข้อมูล Registry ไว้ให้กับผู่อ่าน ซึ่งผู้อ่านสามารถกู้กลับคืนมาได้ โดยการกด F8 ก่อน Load Windows แล้วเลือก "Command prompt only" เพื่อบังคับให้เข้าสู่ DOS ก่อน จากนั้นพิมพ์คำสั่ง Scanreg /Restore จะมีรายชื่อ Registry เก่าที่สำรองไว้ขึ้นมาให้เลือก ให้ผู้อ่านเลือกจาก Registry ที่ใกล้เคียงกับชุดปัจจุบันที่สุดก่อน แล้วลองใช้ดู หากยังไม่ได้ผล ก็ให้ย้อนไปที่ Registry ตัวที่เก่าลงตามลำดับ อย่างไรก็ตาม Registry ชุดเก่าอาจยังไม่ได้บรรจุค่า Key ของบางโปรแกรมที่ติดตั้งลงไปหลังจากสำรอง Registry ชุดนั้น อาจทำให้โปรแกรมดังกล่าวทำงานได้ไม่สมบูรณ์ ผู้อ่านก็ทำการติดตั้งโปรแกรมนั้นอีกครั้ง

5. Registry เสียไม่สามารถแก้ไขได้ และในชุด Restore ก็เสียด้วย วิธีนี้ไม่สามารถกู้ได้เลย ยกเว้นกรณีที่คุณได้มีการสำรอง Registry เอาไว้ โดยการใช้โปรแกรม Scanreg /Backup ซึ่งจะสำรองไฟล์ Registry ไว้ให้ดีกว่าที่ Scanreg ทำให้เองแบบอัตโนมัติ หรืออาจจะใช้เมนู Export ของ Regedit ส่งออกมาเป็น Text ไฟล์นามสกุล *.Reg ก็ได้ แต่ตอนคืนค่าเข้าไปต้องใช้ Regedit บน DOS และใช้คำสั่งบน DOS ซึ่งยุ่งยากกว่า

การแก้ Registry ที่เจาะลึก และซับซ้อนยิ่งขึ้น

การแก้ Registry ทั่ว ๆ ไป นั้น ผู้เขียนสามารถอ่านข้อความตัวแปร Key และ Value ต่าง ๆ เพื่อทำความเข้าใจได้ทันที โดยมากแล้วจะสามารถตีความได้ และจากการทดลองเปลี่ยนค่าไปมา และใช้โปรแกรมตรวจจับดูการเปลี่ยนแปลง จะเข้าใจได้ไม่ยากว่าตรงไหน ทำหน้าที่อะไร อย่างไรก็ตาม บางส่วนของ Registry ก็มีความซับซ้อน เกี่ยวข้องกับเลขฐาน 16 และความรู้เฉพาะทางในด้านที่เราจะแก้ไข เช่น จะแก้ไข Registry เกี่ยวกับ Network ก็ต้องมีความรู้ Network ระดับเจาะลึกลงไปหลาย ๆ ส่วนต้องการความรู้พื้นฐานการเขียนโปรแกรม หรือหลักการทำงานของ Hardware แบบลึก ๆ ลงไป

ผู้เขียนจะแสดงตัวอย่างจริงของการเข้าไปแก้ Registry ด้วยตัวผู้เขียนเอง เนื่องจากว่าคีย์ที่มีอยู่ใน Registry นั้น มีนับแสนคีย์ และเปลี่ยนแปลงตลอดเวลาตามรุ่นของ windows และ โปรแกรมที่ติดตั้งลงไป จากคีย์ทั้งหมด มีคีย์จำนวนมากที่เป็นของระบบที่มีไว้ใช้เอง ไม่มีประโยชน์ที่จะเข้าไปเปลี่ยน เช่น พวกคีย์ที่เกี่ยวกับ Hardware Plug & Play พอเข้าไปเปลี่ยน หลังจาก Boot เครื่องใหม่ก็จะ Detect กลับมาเป็นค่าเดิมอีก หรือกลับส่งผลเสียมากกว่าเดิม เช่นทำให้ Hardware นั้นใช้ไม่ได้ อีกส่วนหนึ่งใน Registry ทาง Microsoft ได้เตรียม Tools ไว้ให้ปรับแก้ได้โดยง่ายอยู่แล้ว Control panel เป็นตัวอย่างหนึ่งของ Tools ที่ใช้แก้ Registry ทุกสิ่งทุกอย่างที่ผู้อ่านแก้ใน Control panel ไม่ว่าจะเป็นระบบเสียบ การแสดงผล Font ต่าง ๆ ล้วนเกี่ยวข้องกับ Registry ซึ่งการแก้ผ่าน Control panel จะปลอดภัยและง่ายกว่า และผลที่แสดงออกมาก็เหมือนกัน ผู้อ่านจึงไม่มีความจำเป็นที่จะต้องรู้ Registry หมดทุกตัว แต่น่าจะมุ่งไปที่ไม่สามารถเข้าไปแก้ผ่าน Interface ธรรมดาที่มากับ windows ได้ แต่หากต้องการรู้จริง ๆ ว่า Tools ไหน สัมพันธ์กับคีย์ไหนใน Registry ก็ใช้โปรแกรม Regmon ตรวจจับการเปลี่ยนแปลง

การเข้าไปแก้ Registry โดยตรงแบบหวังผลนั้น ก่อนอื่น มีตัวย่อที่ผู้อ่านต้องรู้ก่อน เมื่อผู้อ่านไปอ่าน Help หรือใช้งาน Utilities ผู้อ่านจะพบ HIVE และตัวย่อดังต่อไปนี้

```
HKCR  = HKEY_CLASSES_ROOT
HKCU  = HKEY_CURRENT_USER
HKLM  = HKEY_LOCAL_MACHINE
HKU   = HKEY_USERS
HKCC  = HKEY_CURRENT_CONFIG
HKDD  = HKEY_DYN_DATA
```

Windows 95 Registry Binary Value Reference List

ยังมีอีกเรื่องหนึ่งที่ผู้เขียนอยากให้ผู้อ่านรู้เกี่ยวกับ Registry ก็คือ CLSID (Class ID) หลักการคือWindows มองทุกอย่างในระบบเป็น Object โดยที่แต่ละ Object มี Class ของตัวเอง ซึ่งหากผู้อ่านพยายามเข้าไปแก้ไข Control panel แล้วหาไม่เจอ ก็เนื่องจาก Control panel ใน Registry นั้น ถูกเก็บและอ้างอิงในรูปของ Class ใช้เป็นตัวเลขยาว ๆ แทน ดังนั้น หากผู้อ่านต้องการเข้าไปจัดการกับ Object ไหนใน Windows ก็ต้องค้นหา หากรู้เลข class id แล้วก็จะรู้ว่า Object นั้น ๆ อยู่ที่ไหน แล้วก็ค่อยหาวิธีจัดการอีกที object เหล่านี้ถูกเรียกใช้จากหลายที่ในส่วนของ Registry

ผู้อ่านลองเข้าไปดูที่HKEY__LOCAL__MACHINE\Software\CLASSES\CLSID\ จะพบ Object ต่าง ๆ เต็มไปหมด พอรู้ตำแหน่งใน Registry ก็ไปแก้ ไอคอน ลูกเล่นต่าง ๆ จากตัวอย่างผู้อ่านอาจจะทดลองโดยใช้ Regedit และ Find โดยนำตัวเลข CLSID ใส่เข้าไปค้นดู เมื่อเจอแล้วก็จดตำแหน่งไว้ แล้ว Find next ไปเรื่อย ๆ จะเห็นความสัมพันธ์กันของ Object ใน Registry นอกจากนี้ ผู้อ่านยังสามารถใช้ภาษาเช่น VB เขียนโปรแกรมเข้าไปแก้องค์ประกอบของ Windows ได้โดยผ่าน Registry นั่นเอง

ส่วนหนึ่งของ Object ของ Windows

```
Control Panel {21EC2020-3AEA-1069-A2DD-08002B30309D}
Printers {2227A280-3AEA-1069-A2DE-08002B30309D}
Recycle Bin {645FF040-5081-101B-9F08-00AA002F954E}
My Computer {20D04FE0-3AEA-1069-A2D8-08002B30309D}
Net. Neighborhood {208D2C60-3AEA-1069-A2D7-08002B30309D}
Inbox {00020D75-0000-0000-C000-000000000046}
Desktop {00021400-0000-0000-C000-000000000046}
Shortcut {00021401-0000-0000-C000-000000000046}
```

Subkey ใน Hkey_Local_Machine

Config เป็นที่รวบรวมและจัดเก็บ Configuration ทั่ว ๆ ไปของเครื่อง Computer

Enum ข้อมูลเกี่ยวกับ Hardware ที่มีอยู่ในเครื่อง

Network ถูกสร้างขึ้นเมื่อผู้ใช้ Logon สู่เครือข่าย

Security ระบบความปลอดภัย และระบบ Remote Administration

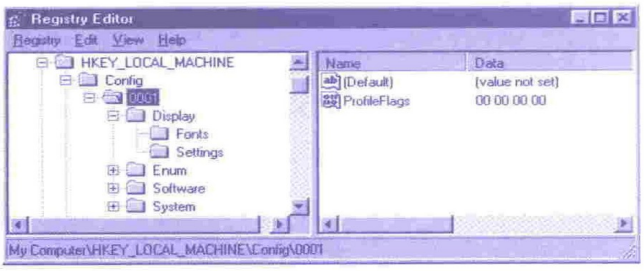
Software ข้อมูล Software ในระบบ และค่าที่ปรับแต่ง

System ควบคุมการ Start-up , การ Load driver , และกำหนดการทำงานหลายอย่างของ OS

Hkey__Local__Machine\Config (ดังรูปที่ 6)

เก็บข้อมูลตัวแปร และค่าต่าง ๆ ของ Hardware มีความสามารถเก็บค่าแตกต่างกันได้ตามความเหมาะสม เช่นเก็บค่าหนึ่ง สำหรับใช้ขณะเชื่อมต่อกับ Network อีกค่าหนึ่งสำหรับสภาวะปกติ วิธีนี้ทำให้ Windows บนคอมพิวเตอร์เครื่องเดียวกันสามารถจะมีคุณสมบัติแตกต่างกันไปตามช่วงเวลาการใช้งาน และความต้องการของผู้ใช้ โดยจะเก็บค่าในรูปของ Key ย่อย ใน Key "Config" อีกทีซึ่งจะตั้งเป็น ID ขึ้นมา เช่น "0001" ค่าต่าง ๆ ใน Key นี้ คือค่าที่เห็นใน Hardware profiles ใน System Icon ของ Control panel นั่นเอง

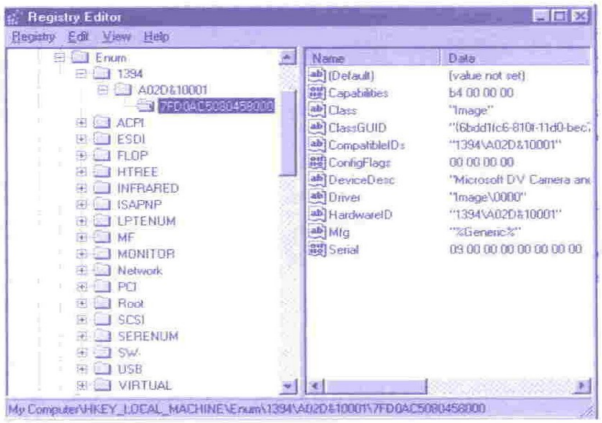
เมื่อขณะที่กำลัง Load Windows ขึ้นมา จะมีการเลือก ID ที่เหมาะสม หากผู้อ่าน Logon สู่ Network ก็จะเลือกค่าสำหรับ Network ให้ระบบนี้เป็น Plug and play แน่นอน หากมี Hardware ใหม่ในระบบจะตรวจสอบ และติดตั้งค่าที่เหมาะสมให้โดยอัตโนมัติ



รูปที่ 6

Hkey__Local__Machine\Enum (ดังรูปที่ 7)

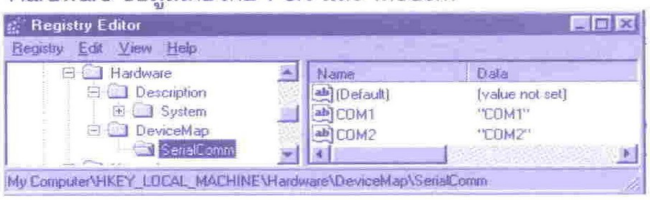
Windows bus enumerators ทำหน้าที่สร้างรายชื่อ Hardware ทั้งหมด รวมทั้งเก็บค่า ID และรายละเอียดทั้งหมดของ อุปกรณ์ Hardware นั้น ๆ ซึ่งเลข ID นี้อาจได้มาจากอุปกรณ์ หรือ Registry เป็นผู้กำหนดให้ก็ได้



รูปที่ 7

Hkey__Local__Machine\Hardware (ดังรูปที่ 8)

Hardware ข้อมูลเกี่ยวกับ Port และ Modem



รูปที่ 8

Hkey__Local__Machine\Network

ข้อมูลตรงนี้จะถูกสร้างเมื่อผู้ใช้ Logon เข้าสู่เครือข่าย ซึ่งจะมีข้อมูลชื่อของผู้ใช้เครือข่ายหลักและข้อมูลpolicy

Hkey__Local__Machine\Security

เกี่ยวกับระบบความปลอดภัยของเครือข่าย และสิทธิการทำ Remote administration

Hkey__Local__Machine\Software

เป็นที่เก็บ Registry ของ Software ทั้งหลายที่ติดตั้งลงสู่ระบบ ซึ่งการที่ software จะมารวมใช้ Registry ที่เดียวกันเช่นนี้ เป็นประโยชน์ต่อการแลกเปลี่ยนข้อมูลระหว่างโปรแกรม (OLE) การปรับแต่งค่าต่าง ๆ ใน Registry ส่วนใหญ่จะมีลูกเล่นกันตรงนี้ ซึ่งในส่วนนี้จะมี Key ย่อยอีกจำนวนมาก ขึ้นอยู่กับจำนวนโปรแกรมที่ติดตั้งลงไปด้วย อย่างไรก็ตาม มี Key ย่อย สำคัญ ๆ ที่น่าสนใจ ได้แก่

HKEY__LOCAL__MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall เก็บรายชื่อโปรแกรมที่ติดตั้งอยู่บน Windows สำหรับใช้ถอนโปรแกรม ตามที่ปรากฏใน Section Add/Remove program ใน Control panel

HKEY__LOCAL__MACHINE\Software\Microsoft\Windows\CurrentVersion\run ที่ผู้อ่านสามารถระบุ Path ของโปรแกรมที่ต้องการให้รันทันทีเมื่อเปิด Windows ขึ้นมา ผู้อ่านอาจจะสังเกตเห็นมุมล่างขวาของ windows ของผู้อ่านที่มี โปรแกรมพวก Antivirus Load ขึ้นมาทันทีที่เปิด windows สังเกตว่าโปรแกรมเหล่านี้ไม่ได้ถูกกำหนดโดยใส่ Shortcut เข้าไปที่เมนู Start up นะครับ

HKEY__LOCAL__MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce เหมือนกับ Run แต่จะทำงานเพียงวันละครั้ง เช่นใช้สำหรับโปรแกรมสแกนไวรัส

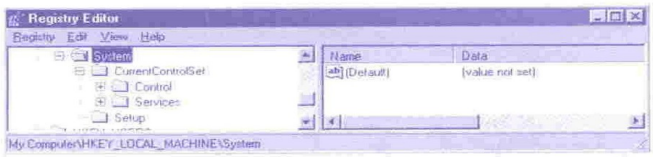
HKEY__LOCAL__MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce ใช้ในกรณีพิเศษ เช่น ในการติดตั้งโปรแกรมบางครั้งจำเป็นต้องติดตั้งทับไฟล์หลักของ Windows ซึ่งผู้อ่านไม่สามารถติดตั้งได้ขณะนั้นเนื่องจาก Windows ใช้งานอยู่ จึงใช้วิธี copy ไฟล์ลงไปใน temp directory จากนั้นเพิ่ม Key ชื่อ "runservices" เข้าไป หลังจากนั้นก็ Reboot ซึ่งในการเข้าสู่ Windows ครั้งถัดมา จะเริ่มด้วยการ Copy ไฟล์ใน Temporary ให้กับ Windows ก่อนแล้วลบ Key runservices" ออก

Hkey__Local__Machine\System (ดังรูปที่ 9)

ข้อมูลที่เก็บอยู่ใน Hkey__Local__Machine\System เป็นข้อมูล Device driver และชุดควบคุม รวมทั้ง Service ต่าง ๆ ของ Windowsให้ สังเกตใน HKEY__LOCAL__MACHINE\System\CurrentControlSet มีส่วนที่น่าสนใจอยู่ 2 ส่วน คือ

key "Control" เก็บข้อมูล system startupที่จะใช้ตอนเริ่มระบบ

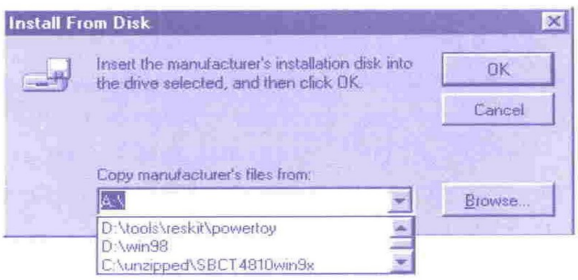
key "Service" เป็นข้อมูลเพื่อควบคุม Configuration ของ driver ระบบไฟล์ รวมทั้งเก็บข้อมูลวิธีการควบคุมการเรียกใช้งานระหว่าง Service ต่าง ๆ ด้วย



รูปที่ 9

ตัวอย่างคีย์ที่น่าสนใจ

HKEY__CURRENT__USER\InstallLocationsMRU - เวลาที่ผู้อ่านติดตั้งโปรแกรม และมีการเรียกหาไฟล์ ตัวติดตั้งจะมี Doalog box ขึ้นมาให้ Browse หาตำแหน่งของไฟล์ต้นทางที่จะติดตั้ง ผู้อ่านจะเห็นในช่องที่กำหนด Folder ที่เรียกใช้บ่อย ๆ มาให้แล้วเพื่อความสะดวก (ดังรูปที่ 10)



รูปที่ 10

HKEY__LOCAL__MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths - ส่วนนี้สำหรับเก็บ Path ของโปรแกรมต่าง ๆ โดยการใส่ชื่อและ Path ของโปรแกรมของผู้อ่านลงไป จะทำให้สามารถเรียกโปรแกรมนั้นโดยพิมพ์เฉพาะชื่อโปรแกรมโดยกดปุ่ม Start/Run... ได้ (คล้าย ๆ กับคำสั่ง Path ใน Autoexec.bat แต่ส่วนนี้เป็นของ Windows)

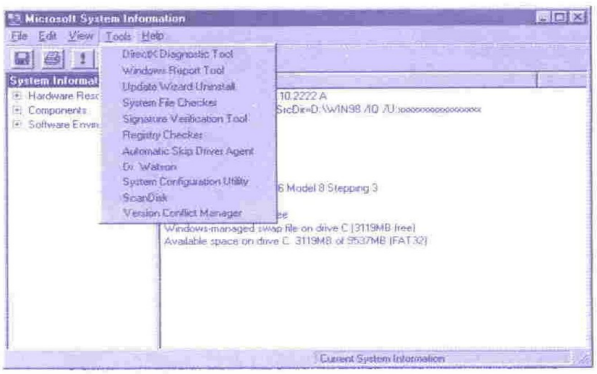
HKEY__CLASSES__ROOT\Folder\shell ถ้าเปลี่ยน Default Value ของ Key นี้เป็น "Explore" เวลาที่เรา Double click ที่ไอคอน My computer จะเปิด Windows Explorer ขึ้นมาแทน ส่วน My computer แบบเดิมจะกลายเป็น shortcut เมื่อคลิกขวา Open

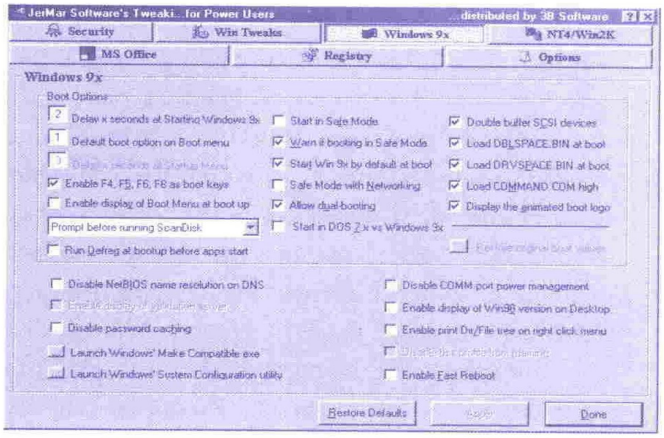
HKEY__USERS\.DEFAULT\Control Panel\Desktop\WindowMetrics เป็นที่เก็บค่าการแสดงผลของผู้ใช้คนปัจจุบัน สามารถปรับแต่ง Interface เช่น Icon, Caption ต่าง ๆ ตรงนี้ได้

อาจสรุปได้ว่า Registry เกี่ยวกับ MS Windows เอง ส่วนใหญ่จะเก็บอยู่ที่ HKEY__LOCAL__MACHINE\Software\Microsoft\Windows มีอะไร ๆ เยอะแยะให้ปรับแต่งเป็นเดือน ๆ ก็ไม่หมด ลองดูนะครับ

7 โปรแกรมหากิน

RegSystemInfo. โปรแกรมนี้ มีมาพร้อมกับ windows อยู่แล้ว ใช้งานง่าย ประสิทธิภาพไม่สูงนัก ข้อดีคือ สะดวก เวลาออกไปซ่อมเครื่องนอกสถานที่ หรือแก้ปัญหาเฉพาะหน้า โดยที่ผู้อ่านไม่ได้เตรียมโปรแกรมอื่นที่มีประสิทธิภาพสูงกว่านี้ไปด้วย วิธีใช้ก็โดย click ปุ่ม Start จากนั้นก็เลือก Programs/Accessories/System Tools/System Information เมื่อเปิด System Information ขึ้นมาได้แล้ว ก็ให้เลือกที่เมนู Tools / Registry Checkerดังรูปที่ 11 ก็คือ Tweak นั่นเอง แต่มีความสามารถเหนือกว่า Tweak UI ที่มากับ Resource Kit ของไมโครซอฟท์ ผู้อ่านสามารถใช้โปรแกรมนี้ตั้งค่าต่าง ๆ ของ Windows แบบเจาะลึก ตั้งแต่กำหนดวิธีการ Boot เครื่อง เกี่ยวกับความปลอดภัยของ Network , Cache , จัดการกับไฟล์ Temp และ Config ต่าง ๆ ปิด/เปิด ปุ่ม และ ไอคอนต่าง ๆ บน Windows และเก็บ List รายชื่อ path หรือ ไฟล์ที่ใช้บ่อย นอกจากนี้ ยังมีความสามารถปรับแต่ง Registry ในส่วนของ MS Office และ IE ได้อีกด้วย ที่จริงแล้ว การแก้ไขค่าต่าง ๆ เหล่านี้สามารถจะเข้าไปแก้ไขเองก็ได้ใน Regedit แต่โปรแกรมนี้ทำสำเร็จรูปมาให้สะดวกในการใช้



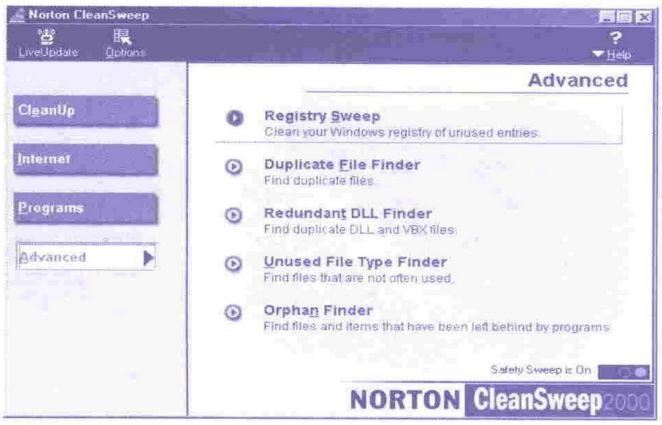


รูปที่ 11

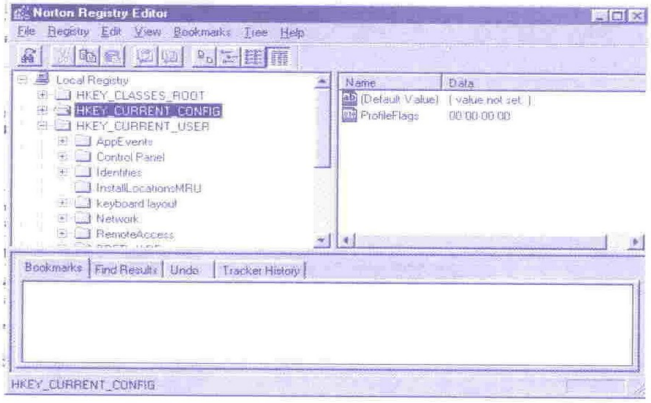
รูปที่ 12 หลายคนคงรู้จักโปรแกรม Clean sweeper เป็นอย่างดี ในฐานะเป็นโปรแกรม Uninstall ที่ยอดเยี่ยม จริง ๆ แล้ว Cleansweeper ยังมีความสามารถในการจัดการกับ Registry ได้ด้วย บ่อยครั้งที่ผู้อ่านยกเลิกโปรแกรมแบบ Manual หรือโปรแกรมที่ยกเลิกไม่เกลี้ยง ทำให้เกิดขยะขึ้นใน Registry ได้

ขยะเหล่านี้ ทำให้การ Load Registry ทำได้ช้า Load Windows ก็ช้าไปด้วย ในกรณีที่แย่กว่านี้ ก็ทำให้เกิดกรอบข้อความเตือนว่าไม่สามารถหาไฟล์ใดไฟล์หนึ่งพบ ให้กด OK และที่หนักไปกว่านั้นก็คือ ตอน Boot จะขึ้นข้อความเตือนทำนอง " Error VKD" โปรแกรมนี้แม้จะไม่สามารถซ่อม Registry แต่ก็สามารถกำจัดขยะใน Registry ได้เป็นอย่างดี โดยการเข้าไปตรวจสอบว่ามี Key ไหนบ้างที่ไม่ได้ใช้งาน พร้อมทั้งวิเคราะห์เสร็จว่า Key ไหนปลอดภัยหรือไม่ที่จะลบทิ้ง ผู้เขียนเองใช้โปรแกรมนี้บน windows NT ด้วย ก็ได้ผลดีเวลาที่ผู้เขียน Cloning Harddisk จากเครื่องหนึ่งมานั้น NT เครื่องของผู้เขียนไม่สนับสนุน Plug and Play ผู้เขียนก็ติดตั้ง NT ทับ แล้วใช้โปรแกรม Clean sweep นี้เข้าไปลบขยะ Registry และ Error จากการหา Device ที่ไม่เจอออกได้อย่างมีประสิทธิภาพ

รูปที่ 12



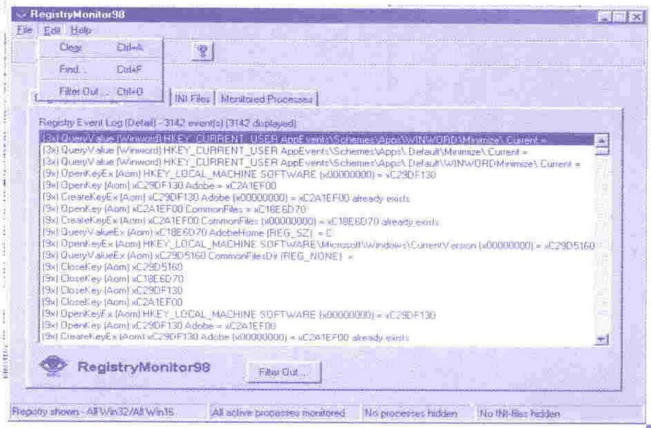
จากรูปที่ 13 เหนือกว่า RegEdit ที่มีมากับ Windows โปรแกรม Norton Registry editor ให้ความสามารถมากกว่าในการจัดการกับ Registry สำหรับคนที่ใช้ Regedit มาแล้ว จะพบว่ามีหน้าตาคล้าย ๆ กัน แต่ Norton ทำได้ดีกว่าในแง่ของการแยกแยะสีสัน ความแตกต่างของ Key และ Value ต่าง ๆ ใน Registry แสดง win.ini และ system.ini ให้พร้อมกันด้วยในคราวเดียว สนับสนุนการระบุตำแหน่ง Bookmark ในขณะที่ให้ความสามารถทางด้าน Network registry เช่นที่ใน Regedit ที่ผู้เขียนชอบมากจนยกนิ้วให้คือ มี History ให้ด้วย เวลาแก้ไขแก้ไปแก้มาเผลอลบ หรือผิดพลาด สามารถย้อนกลับมาได้ โปรแกรม Registry editor ของ Norton นี้ มีมากับชุด Norton Utilities 2000-2001ครับ



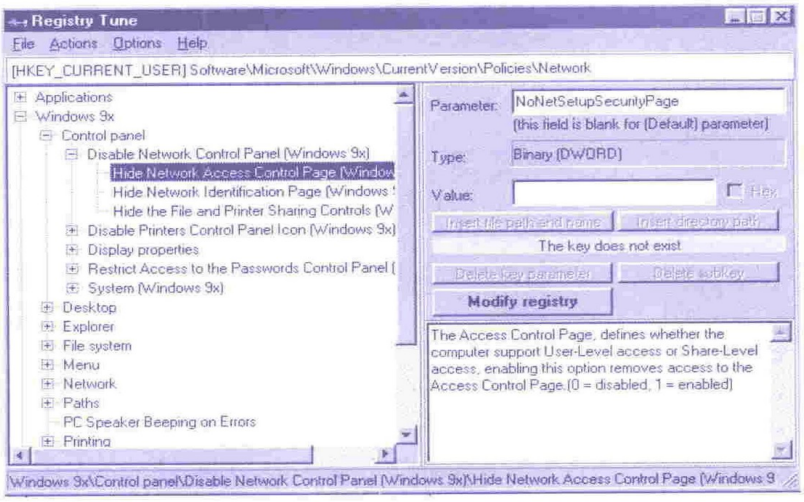
รูปที่ 13

จากรูปที่ 14 ใช้เพื่อที่จะตรวจจับความเคลื่อนไหวของ Registry แบบ Realtime สามารถตรวจจับการเปลี่ยนแปลงต่าง ๆ ที่โปรแกรมในวินโดวส์ที่เขียนลงไปได้อย่างมีประสิทธิภาพ เมื่อเราสามารถดักดูการทำงานได้แล้ว ความลับของ Registry ก็ไม่ลับอีกต่อไป ผู้เขียนเคยเห็นพวกนักศึกษาโปรแกรมหลาย ๆ ท่านใช้โปรแกรมนี้ช่วยในการศึกษา Evaluation copy ของโปรแกรมต่าง ๆ โดยอาศัยหลักการว่า โปรแกรมเหล่านั้นเขียนค่าการป้องกัน และกำหนดอายุการใช้งานเข้าไปใน Registry เมื่อค้นพบว่าโปรแกรมไปตรวจสอบหรือเขียน Registry ที่ไหนแล้ว ก็ไม่ยากที่จะเขียน Key generator หรือตัวกำเนิดเลขรหัสลงทะเบียนขึ้นมา

รูปที่ 14

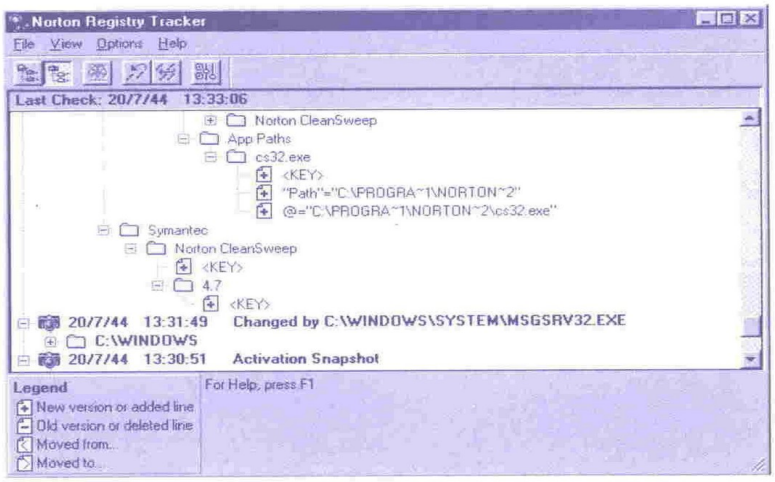


จากรูปที่ 15 หนึ่งในโปรแกรมที่รวบรวมค่าต่าง ๆ ใน Registry ที่น่าสนใจมาทำเป็น Interface ที่ง่ายสำหรับผู้อ่าน ทำให้ไม่ต้องมีความรู้เรื่อง Registry มากนักในการปรับแต่ง ทั้งยังปลอดภัย และมีคำอธิบายรายละเอียดของพารามิเตอร์ต่าง ๆ ใน Registry ให้อีกด้วย โปรแกรมนี้ ช่วยในการปรับแต่ง ทำให้ผู่อ่านไม่ต้องเข้าไปแต่งใน Regeditเอง บางทีการปรับแต่งอาจจะมีอยู่ในหลายตำแหน่งใน Registry ซึ่งสัมพันธ์กัน เป็นการเสี่ยงสำหรับผู้ที่ไม่ชำนาญ Registry จริง ๆ ถ้าเข้าไปปรับแต่งอาจจะทำให้เสียหายได้ ในการใช้งานโปรแกรมนี้ ผู้อ่านสามารถปรับซ่อน/แสดง ไอคอน ที่สำคัญเช่นใน Network, Password จัดการเกี่ยวกับไฟล์ , Cache และค่าต่าง ๆ ของระบบ Windows การ Logon เข้าระบบ ปิดการทำงานของเมนู และการแสดงผลต่าง ๆ นอกจากนี้ยังสามารถเข้าไปแก้ไขใน Regisrty ของ WindowsNT ได้อีกด้วย



รูปที่ 15

จากรูปที่ 16 โปรแกรม Registry Tracker จากบริษัท Norton เป็นหนึ่งใน Utilities เกี่ยวกับ Registry ที่ทรงอานุภาพสามารถหาได้โดยโปรแกรมนี้เป็นหนึ่งในโปรแกรมที่อยู่ในชุดของ Norton Utilities 2000-2001 คุณสามารถทำ Snapshot กล่าวโดยเปรียบเทียบได้กับการที่เราตั้งกล้องตรวจจับไว้ว่ามีการเปลี่ยนแปลง Registry ตรงไหนบ้างในระบบ โปรแกรมนี้ต่างจากโปรแกรม Registry monitor ตรงที่ Registry monitor ใช้จับการเปลี่ยนแปลงแบบ Real time แต่ Registry tracker จะดู Registryทั้งหมดโดยรวมแล้วแยกแยะให้ด้วยว่าเป็นการเพิ่ม ลบ หรือแก้ไข Registry ตรงส่วนไหนบ้างอย่างไร ตัวอย่างการประยุกต์ใช้ก็โดยการเปิดโปรแกรมตั้ง Snap shot ไว้ก่อน จากนั้นติดตั้งโปรแกรมใหม่ หรือลองปรับเปลี่ยนค่าในโปรแกรมดู เจ้าโปรแกรม Registry Track จะฟ้อง พร้อมทั้งแยกแยะให้เราเลยว่าอะไรเปลี่ยนไปตรงไหนบ้าง ดังที่กล่าวมาแล้วว่า เรื่องราวเกี่ยวกับ Registry นั้นกว้างใหญ่ไพศาล ผู้เขียนจึงเน้นให้ข้อมูลในส่วนที่ผู้อ่านสามารถไปศึกษาหาความรู้เองได้เป็นหลัก ตรงจุดของ Registry tracker นี้ ผู้อ่านสามารถศึกษาได้เองด้วยว่า Registry ทำงานอย่างไร แล้วจะค้นพบความมหัศจรรย์ที่ซ่อนอยู่อีกมาก ผู้เขียนใช้โปรแกรมเหล่านี้เป็นส่วนในการค้นคว้าและเขียนบทความนี้ ผู้อ่านจะลองเข้าไปแก้ค่าต่าง ๆ ใน control panel ดูก็ได้ แล้วดูผลว่า Registry และไฟล์ ini ถูกแก้ไขอย่างไร โปรแกรมเหล่านี้หาซื้อได้ทั่วไปที่พันธุ์ทิพย์ก็มีเยอะครับ สำหรับโปรแกรมที่เป็น Shareware หายากหน่อย ผู้เขียนเตรียมไว้ให้ที่ www.pantipweb.com ครับ สุดท้ายนี้ผู้เขียนขอจบบทความเรื่องราวเกี่ยวกับ Registry ไว้เพียงเท่านี้ก่อนนะครับ ไว้พบกันใหม่ในฉบับหน้า สวัสดีครับ



รูปที่ 16